UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,541	11/17/2005	Daniil Utin	13984-005US1	6860

26161 7590 03/25/2011
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
ZIA, SYED	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
03/25/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Attachment to Advisory Action

This office action is in response to amendment and remarks filed on March 7, 2011. Claims are 1-12 are pending for further consideration.

Response to Arguments

Applicant's arguments filed on March 7, 2011 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims applicants previously argued that the cited prior arts (CPA) [Challener et al. (U. S. Patent 6,718,468)] " Challener simply uses a public/private key, which is not described as being produced from user supplied information, to encrypt a password (and the encrypted password is stored). At a later time, the encrypted password is retrieved, de-encrypted and compared to another password from a user (presumably provided to gain access to a system, for example). However, nowhere does Challener disclose or suggest "generating a first key from a user-supplied unencrypted password provided by a user computing device" and "encrypting the user-supplied unencrypted password using the key", as required by independent claim 1 ".

This is not found persuasive. In the system of cited prior art teaches during operation, a first pass phrase sent by a user is **hashed** by a processor, such as processor 12 in FIG. 1, in a system memory, such as RAM 14 in FIG. 1, to obtain its corresponding first password. Thus, a first password is generated by hashing a first pass phrase, as shown in block 45. This first password along with the encrypted package of the first password and random password (from the

hard disk) are then sent to the signature chip. The signature chip decrypts the encrypted package of the first password and random password. The signature chip then compares the first password from the decrypted package of the first password and random password with the sent first password (col.4 line 30 to line 54).

The system of cited prior art teaches a associating method in computer system to associate password and secured user public/private key pair, which involves accessing user private key using primary/secondary phase phrases for performing authentication function. After encrypting established user private key with random password, primary/secondary passwords are generated by hashing the primary/secondary pass phrases. The user private key is accessed using primary/secondary phase phrases, for performing authentication function, after performing encryption of random password with the generated primary/secondary passwords, respectively (col. 3 line 55 to col.5 line 24).

As a result, cited prior art does implement and teach a system that relates to generating of password-encrypted key form a user-supplied password (pass phrase) and stored in a temporary storage to maintain an access to a secure network communications and access a network (Fig.2a-2b).

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 1-12 are respectfully maintained.